METHOD AND APPARATUS FOR AUTHENTICATING SERVICE TO A WIRELESS COMMUNICATIONS DEVICE

FIELD OF THE INVENTION

[001] The present invention relates to authenticating service to a wireless communications device. The invention relates particularly to authenticating use of hotspot wireless communications device services provided by a wireless network.

BACKGROUND OF THE INVENTION

[002] It has been predicted that wireless local area networks (WLANs) will soon provide a significant proportion of the wireless access to computer networks and/or the Internet via "hotspots", which enable a user to have wireless connection by radio frequency (RF) communication to a computer network when the user is in a designated area forming the "hotspot". The hotspots may form part of a cellular telecommunications network and may be an extension of the existing cellular telecommunication networks already widely available.

[003] A problem with accessing WLANs via hotspots is that a user may be unaware of the suitability of the provider of a particular hotspot. Similarly, the provider of a hotspot may have problems in determining whether a request for use of the hotspot by a user should be accepted.

[004] In the following a hotspot is an area where a wireless communication to a WLAN can take place, the area being geographically limited to being approximately tens of metres in size. Several hotspots may be created together in a cluster to serve a site having a size larger than a single hotspot, such as an airport, hotel, conference centre, office building or the like. A hotspot typically allows access to services or information etc on the Internet.

SUMMARY OF THE INVENTION

[005] According to a first aspect, the present invention provides a method wherein a cellular communications service provider authenticates a provider of a service running at a wireless hotspot. The method comprises receiving an indication of potential use of a specified wireless hotspot from a user. The trustworthiness of the

provider of the service is verified with a party independent from said service provider. On successful verification of the provider of the service, the user is provided with a confirmation that the provider of the service is authenticated by the cellular communications service provider.

[006] According to a second aspect, the invention provides a computer system for a cellular telecommunications provider. The system comprises a processor adapted to: (1) receive an indication of potential use of a specified wireless hotspot from a user; (2) identify services available at the specified wireless hotspot; (3) authenticate providers of the services available at the specified wireless hotspot; and (4) prepare authentication information for use to the user.

[007] According to a third aspect, the invention provides a method wherein a cellular telecommunications provider authorises a user to use a location-dependent service. The method comprises: tracking the location of a user via a wireless communications device of the user; determining that the user is or will be within an operating range of the location-dependent service; authenticating a provider of the service; and providing authentication of the provider of the service to the user.

[008] In further aspects, the invention provides appropriate apparatus, and provides suitably programmed computers and data carriers carrying code adapted to program computers suitably.

BRIEF DESCRIPTION OF THE DRAWINGS

[009] For a better understanding of the invention and to show how the same may be brought into effect, specific embodiments will now be described, by way of example, and with reference to the accompanying drawings, in which:

[0010] Figure 1 is a flow diagram of a preferred method of certifying a hotspot user; and

[0011] Figure 2 is a schematic diagram of a user and a WLAN hotspot.

DETAILED DISCUSSION OF THE DRAWINGS

[0012] It is predicted that wireless local area networks (WLANs) will soon provide a significant proportion of the wireless access to the Internet via hotspots. A method is described herein with reference to Figure 1 whereby a user can certify the trustworthiness of a WLAN hotspot provider by using another trusted party, such as a cellular communications service provider.

[0013] The method described in relation to Figure 1 demands that a WLAN hotspot provider and service providers providing services over the WLAN hotspot are vetted, i.e., certified, by, for example, a cellular telecommunications provider. This could apply to a cellular telecommunications provider of any type (including GSM, GPRS and 3G providers). The WLAN hotspot provider and service provider are to be vetted as bona fide companies with whom the cellular telecommunications service provider allows users of its services to communicate. It is possible that in the limiting case, the cellular telecommunications service provider could also be the WLAN hotspot provider, in which case the cellular provider would obviously always positively vet itself.

[0014] The method works as follows.

[0015] In Figure 1 a user enters a WLAN hotspot during operation. The user is typically unsure of a service running at the hotspot – either the trustworthiness of the WLAN operator or of a service provider providing further services over the WLAN hotspot. The user then contacts his cellular telecommunications service provider during operation – this telecommunications service provider being trusted by the user to at least some extent. The contact is made by a user placing a data call with a cell phone to the cellular telecommunications service provider. The call is generally made automatically once the user expresses interest in using the hotspot by pressing - for instance - a "YES" button on his cell phone. The cell phone then sends its location information and the details of the hotspot service provider to the cellular telecommunications service provider. If the cellular telecommunications service

provider has certified the hotspot provider at that particular location then the response back to the user cell phone would be affirmative to use that hotspot and provider.

[0016] The request for certification of the service can be initiated in other ways than manual confirmation of the user as described above. As will be described below, awareness of the existence of a local service may be enough to trigger a certification/authentication step from the cellular telecommunications service provider. Alternatively, the user's cellphone may be adapted such that it cannot use WLAN services (any WLAN services, or WLAN services of a particular type) without confirmation from the cellular telecommunications service provider or its designate if the service provider verifies that the WLAN service concerned is legitimate. This confirmation can be provided, for example, in the form of a key to activate the relevant functionality at the cell phone (use of keys in such authentication is described further below). The cell phone may be adapted so that such confirmation of certification or authentication is always required before use of a WLAN service of the relevant type, or may be adapted so that this could be overridden by the user (who would then, in effect, be taking responsibility for making the security decision about the WLAN services himself or herself).

[0017] The trusted cellular telecommunications service provider is aware of the location of the user by virtue of the request made, since the user location is an integral part of cellular telecommunications. Furthermore, more specific location information can be obtained to give the position of a user within a particular cell using signal strength in adjacent cells to triangulate a user's location. More detail of this can be obtained from Cambridge Positioning Systems (UK) (see www.cursor-system.com /sitefiles/cursor/tech_eotd.htm), Signalsoft (see www.signalsoftcorp.com/products/ index .html), or Cell-loc (see www.cell-loc.com/how_tech.html). Thus the movements of a user or potential user can be tracked.

[0018] It is also likely that the trusted cellular telecommunications service provider has details of the location of the hotspot, particularly if there is an information sharing agreement between the cellular telecommunications service provider and the hotspot provider. The information is typically tabulated to show a hotspot name, an

owner/operator and a location on a suitable database. Thus, the cellular telecommunications service provider, knowing the location of the hotspot can vet the WLAN hotspot as being offered by a trusted WLAN hotspot provider, by cross-referencing user location with known hotspot location information.

[0019] By using this information, a user is provided in advance with information relating to the location of known hotspots that have previously been vetted by a user's cellular telecommunications or hotspot service provider. The cell phone and the cellular provider know the whereabouts of a given cell phone using location finding technology referred to above. Knowing the location of a cell phone (as described above) the cellular provider lets the user know about hotspots in his/her vicinity. In a more advanced system the cellular operator senses the direction a user is moving (e.g. down a road/motorway) and predictively alert the user to upcoming hotspots.

[0020] Also, information can be provided to a user giving the direction or location of a nearest (or a list of nearest) hotspots that a user may wish to use. This information could easily be derived from a user's location information and hotspot location information, with a difference value being calculated.

[0021] The certification or vetting of the hotspot by the cellular provider (operation 24) can be carried out by a number of methods, a non-limiting example of which is if the hotspot provider or service provider over the hotspot is in a list of approved hotspot providers or service providers held by the cellular telecommunications service provider. It should be noted that the certification or vetting (which may be a simple authentication, or also require the service provider concerned to meet certain criteria) need not be provided by the cellular telecommunications service provider directly, but simply by a party whom the user ultimately trusts. This may be a party or one of a group of parties identified by the user, or a party trusted by the cellular telecommunications service provider (either directly or indirectly).

[0022] If operation 24 positively certifies the hotspot provider, then the trusted cellular telecommunications service provider (during operation 26a) confirms to the user that the user can access the relevant service or services provided at the WLAN

hotspot. This can be a simple confirmation, sent (preferably) over a secure cellular telecommunications link to the user (at operation 28a in Figure 1), advantageously by encrypted communication between cellular telecommunications service provider and user. This could also be a key unlocking the relevant WLAN-related functionality at the cellphone. It could also include a key to provide to the service provider at the hotspot to use the hotspot services. Such a key can be an encrypted sequence, using an existing encryption scheme such as public key infrastructure (PKI). The exchange of keys is a standard technique for authentication. Consider two entities: A and B. A sends a code sequence to B, and asks B to encrypt it with B's secret key. B does so, and sends back the encoded sequence to A. A then checks this against it's own calculated coding of the sequence it sent to B. If both sequences agree then A knows B is authenticated

[0023] Since the cellular telecommunications service provider knows the location of the user and also the hotspot (assuming the information sharing agreement mentioned above is in place) then the vetting of the WLAN hotspot provider and service providers on the WLAN hotspot can be carried out automatically without the user having to make a specific request for verification of the WLAN hotspot. The request for certification would be made automatically as soon as the user requests service from the hotspot.

[0024] If the cellular provider of the user does not positively certify the hotspot during operation 24 as having not been a trusted hotspot provider, the cellular provider derives a signal indicating access to the hotspot is denied (operation 26b) and the user is not given the key (indicated by operation 28b) to prevent use of the hotspot by the user.

[0025] The method described above gives users security and trust in accessing a WLAN hotspot and in the services provided through the WLAN hotspot and inhibits "rogue" hotspot providers. Also, advance information about hotspots that a user is approaching can provide increased confidence to a user, as well as providing a more efficient service. If the cellular service provider with its location-sensing technology locates a user and his direction then the cellular provider can pre-authenticate the

likely hotspots that the user will pass-through on his journey and alert the user to the presence and authenticity of these hotspots.

[0026] The user can access the hotspot and a computer network associated therewith with a cellular telecommunications device, which may be a portable computer, or laptop, a personal digital assistant or other mobile computing device.

[0027] In the environment of Figure 2, a user 10 having a communications device 11 (such as a cell phone, laptop computer, a personal data assistant (PDA) or similar device) is within the hotspot region 12. A hotspot provider 14 using a computer 15 communicates with the hotspot 12, as does a cellular telecommunications service provider 16 using a computer 17, the latter also communicating with the hotspot provider 14. The communication by user 10 and hotspot 14 with the cellular telecommunications provider 16 is done via a node 9 of a cellular telecommunications network 7. Computer 17 of the cellular communications service provider 16, in this arrangement, is programmed to request reception, verification and key transmission.

[0028] The hotspot services described herein and the telecommunications networks are performed using computers, such as computers 15 and 17 above, programmed with suitable software.

[0029] The system and method can also track a user as described above, prior to allowing entry of the user to a building or the like. The building would correspond to the wireless service in the above embodiments. A user would be tracked as he approached the building, and would be allowed access to the building on making a request. The request (or potential request) would be one about which a controller of the building access would be aware, given the tracking of the user. Authentication and certification issues for building services would then be addressed.

[0030] The certification methods described herein address the problem of hotspot services potentially being provided by unknown. Thus a, potentially automatic, method is disclosed whereby vetting, i.e. certifying, of a provider of services at a hotspot is achieved.